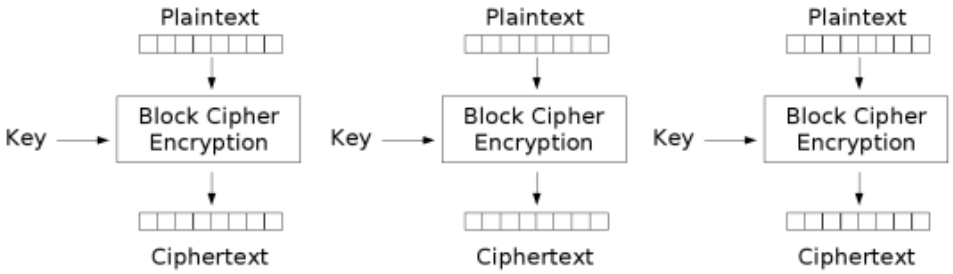
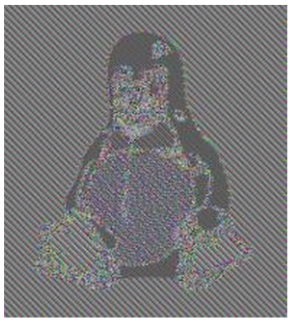
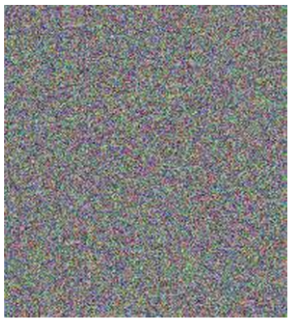
cifrare messaggi lunghi

- Esistono diversi metodi per cifrare messaggi di lunghezza maggiore di un blocco
- Il più semplice è cifrare ogni blocco separatamente con la stessa chiave
- metodo ECB (Electronic CodeBook)



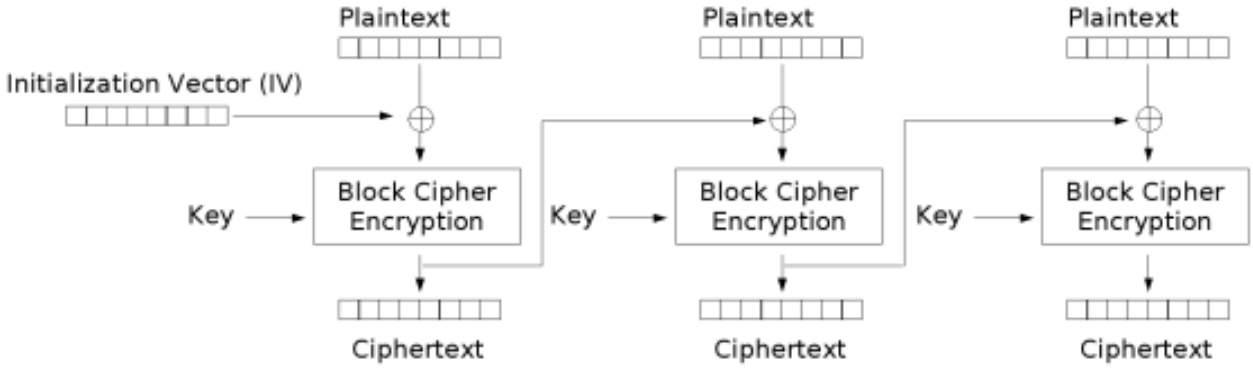
Electronic Codebook (ECB) mode encryption

- Problemi?

- Se due plaintext sono uguali, anche i corrispondenti testi cifrati lo sono (possibili analisi di frequenza).
- 
  Original
  
  Encrypted using ECB mode
  
  Modes other than ECB result in pseudo-randomness
- Un attaccante può inserirsi e cambiare parte del messaggio senza essere scoperto (man-in-the-middle attack).
- Di fatto l'ECB non va mai utilizzato.
- si usano due tecniche per ovviare a questo:
  - Cifratura randomizzata (Randomized encryption)
  - Cifratura basata su un "nonce" (Nonce based encryption)

Cipher Block Chaining

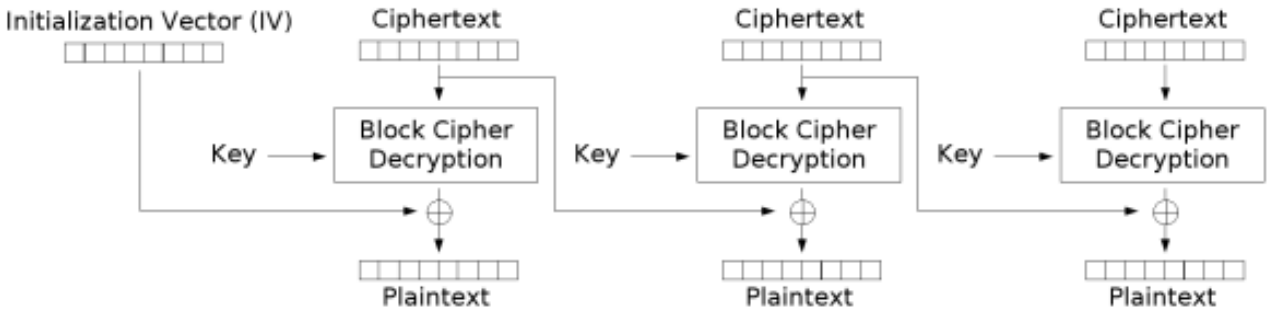
Nel metodo CBC, il plaintext è messo in XOR con il testo cifrato precedente prima di essere cifrato.



Cipher Block Chaining (CBC) mode encryption

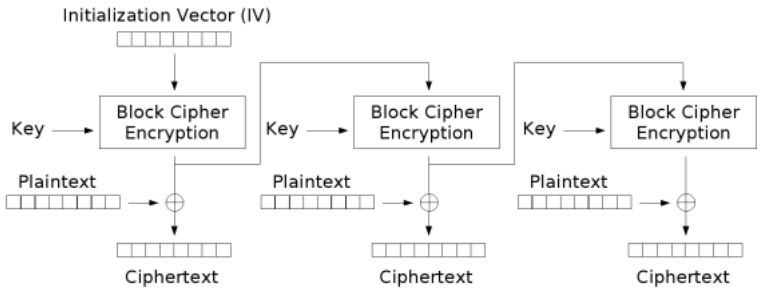
- È una cifratura randomizzata
- Bisogna generare e trasmettere l'IV
- Il CT diventa più lungo del PT: il primo blocco ricevuto saà l'IV
- l'IV non dev'essere segreto, ma deve essere random
- Nasconde eventuali pattern del plaintext
- La lunghezza del PT dev'essere un multiplo della lunghezza di un blocco: si introduce padding

Cipher Block Chaining – decifratura



Cipher Block Chaining (CBC) mode decryption

Output FeedBack



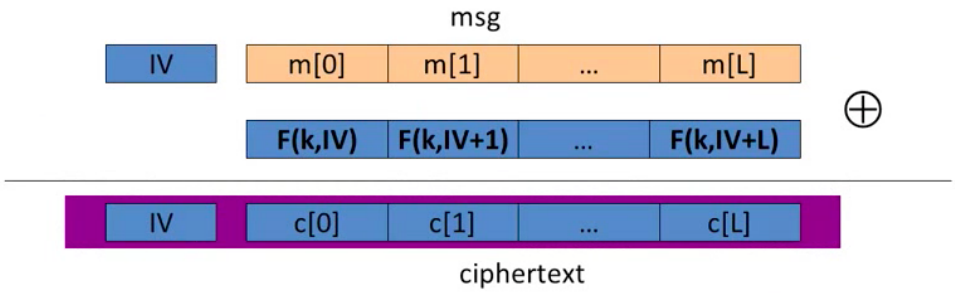
Output Feedback (OFB) mode encryption

- Usa il cifrario a blocchi come un generatore di numeri pseudocasuali.
- Il messaggio è cifrato con uno XOR (OTP)
- la chiave K dell'OTP si ha considerando

$$e_k(IV) = K_0, e_k(e_k(IV)) = e_k(K_0) = K_1, \ldots e_k(K_{i-1}) = K_i$$

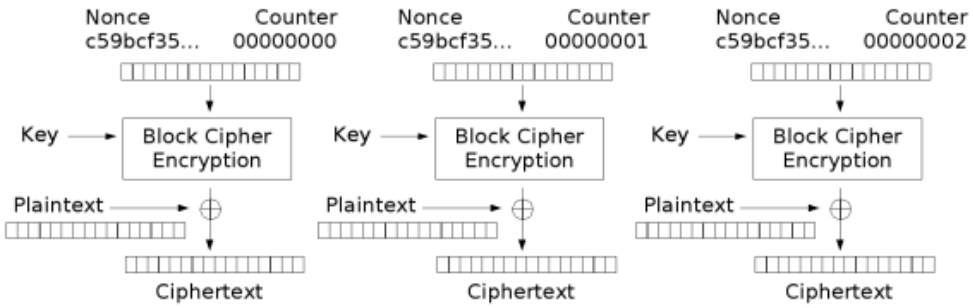
- Posso calcolare questa chiave prima di conoscere il PT da trasmettere

randomized counter mode



- Anche qui si usa il cifrario a blocchi come un generatore di numeri pseudocasuali.
- la chiave K dell'OTP si ha considerando $e_k(IV) = K_0, e_k(IV + 1) = K_1, \ldots, e_k(IV + i) = K_i$
- Posso calcolare questa chiave prima di conoscere il PT da trasmettere e in parallelo.

nonce-based counter mode



Counter (CTR) mode encryption

- invece di un IV random, si considera un nonce concatenato a un counter
- sia nell'OFB che nelle modalità counter, per decifrare si usa solo la cifratura del cifrario a blocchi (per calcolare la chiave OTP)